AMENDMENTS TO THE SPECIFICATION

Please amend paragraphs [0050] and [0051] as follows:

[0050] Once parties are appropriately introduced and validated, a trusted application can establish access between the Secure POP interface level and internal Secure POP security mechanisms (Block 402). These internal Secure POP security mechanisms ("Secure Core") may then generate a user profile referencing the set of expected accesses.

[0051] The Secure Core can include trusted databases of resource providers available through the ~~generate a user profile referencing the set of expected accesses.~~ Secure POP, as well as pre-established access rules created by resource providers. User and resource profiles can then be combined to create a session profile, which represents a set of accesses that are both allowed and expected for a given user in a given session. Session profile data may then be presented to the resource requester as a list of accessible resources (Block 403). In the preferred embodiment, such a list may mask resource provider identities by allowing the Secure Core to maintain a correspondence list in a protected, trusted application. By masking resource provider identities, increased security is provided compared to a conventional resource list. (This may be referred to as data non-attribution, or location hiding by address masking.)